What is Location-Based Application Whitelisting?

For the best balance of performance, security, and manageability, NSA's Information Assurance Directorate (IAD) recommends employing location-based Application Whitelisting rules to both executables and libraries. These location-based rules whitelist large protected locations in file space where many authorized applications may reside without identifying each individual program and library. The locations must be protected so that only authorized administrators can install or modify the files to prevent standard users and malicious activities from circumventing the application whitelisting policy. These rules have a minimal impact on system performance and allow most program updates and patches to be applied without requiring any rule changes, while still preventing the execution of new unauthorized programs and most current malware.

What are AppLocker® and Software Restriction Policies (SRP)®?

AppLocker® is a Windows operating system feature that enforces an administrator defined application whitelisting policy. AppLocker® policies can be created and managed through standard Windows Group Policy management applications and techniques. AppLocker® is available in certain editions of Windows Server 2012, Windows Server 2008 R2, Windows 8, and Windows 7. AppLocker® primarily enhances the functionality of the SRP® feature that was included in Windows XP. Both AppLocker® and SRP® can be used to enforce location-based application whitelisting policies, as well as other forms of application whitelisting.

Where to Find More Information

The IAD's Application Whitelisting guidance documents can be downloaded from:

http://www.nsa.gov/ia/guidance/security_configuration_guides/application%20whitelisting

The documents contain detailed instructions for developing an appropriate whitelist for a Windows network, configuring AppLocker® or SRP®, applying the rules across the network, maintaining the whitelist over time, and monitoring the enforcement of the policy.

The Mitigations Group
National Security Agency
9800 Savage Road, Suite 6704
Fort Meade, MD 20755-6704

MIT-001FS-2013
March 2013

The Information Assurance Mission at NSA

Application Whitelisting

INFORMATION ASSURANCE
DIRECTORATE

What is Application Whitelisting?

Application Whitelisting is a proactive security technique where only a limited set of approved programs are allowed to run, while all other programs (including most malware) are blocked from running by default. In contrast, the standard policy enforced by most operating systems allows all users to download and run any program they choose. Application Whitelisting enables only the administrators, not the users, to decide which programs are allowed to run.

Application Whitelisting is not a replacement for traditional security software, such as antivirus and host firewalls. It should be used as one layer in a defense-in-depth strategy. For an application whitelisting solution to be effective:

- All executable code must be blocked by default so only approved programs can run.
- Users must not be allowed to modify the files that are allowed to run.

All applications have inherent security risks that must be accepted by the organization. However, unauthorized applications have the potential to cause great harm to a computer and to the network to which it is connected. They can introduce unknown and unacceptable additional security risks.

Application Whitelisting prevents the use of unauthorized applications, thereby limiting the attack surface to only security risks that the organization has chosen to accept.

Advantages

- Blocks most current malware
- Prevents use of unauthorized applications
- Does not require daily definition updates
- Requires standardized process for administrator installation and approval of new applications

Disadvantages

- May require performance overhead to enforce the whitelist (varies greatly depending on implementation)
- Requires regular maintenance of the whitelist to add new applications and remove ones that are no longer approved
- Requires a change in user behavior because they can no longer download and run applications at will

Why use Application Whitelisting?

The amount of malware increases in volume and variety every day. Malware developers and antivirus vendors are in a never-ending arms race. Malware authors continuously modify their creations so they are not detected, and antivirus vendors update their software daily to detect new malware variants. Defending against these threats by blocking every known malware sample, a technique known as *blacklisting*, is a reactive technique that does not scale well to the increasing volume and variety of malware. It also does not protect against unknown malware. Many attacks use previously unknown malware, which cannot be prevented with blacklisting techniques.

Corporate and government networks are prime targets for attackers. They contain valuable proprietary or sensitive information and have a large, diverse attack surface for an adversary to exploit. Attacks have shifted from operating system attacks to application-based attacks. This change has left each individual user, and the applications they use, as the main attack vectors into the network.

How to Enforce Application Whitelisting

There are several vendors that offer enterprise Application Whitelisting solutions. Most of the solutions make management of the whitelist easy for administrators, enable updating of applications, and monitor and report attempted violations of the policy. Many of these solutions are expensive, unlike the built-in (no additional cost) AppLocker® or Software Restriction Policies (SRP)® features on Windows computers. Additionally, application control capabilities are included in some Host Intrusion Prevention System (HIPS) products and host-based security suites.